PCT/JP2004/006440

26. 5. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月１７日

出願番号
Application Number: 特願２００３－３８７２１３

[ST. 10/C]: [ＪＰ２００３－３８７２１３]

出願人
Applicant(s): 株式会社インテリジェントウェイブ

２００４年 ５月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００４－３０４１６６７

【書類名】　特許願
【整理番号】　P03-57
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　青木　修
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　白杉　政晴
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　小出　研一
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　河野　裕晃
【特許出願人】
　【識別番号】　397067853
　【氏名又は名称】　株式会社インテリジェントウェイブ
【代理人】
　【識別番号】　100117592
　【弁理士】
　【氏名又は名称】　土生　哲也
【手数料の表示】
　【予納台帳番号】　146663
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定システムであって、
前記オペレーションを実行するためのデータを受け付けるオペレーション受付手段と、
前記データから前記コンピュータにかかる第一のプロファイルを作成する第一のプロファイル作成手段と、
前記第一のプロファイルを格納する第一のプロファイル格納手段と、
前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成する第二のプロファイル作成手段と、
前記第二のプロファイルをユーザ別に格納する第二のプロファイル格納手段と、
前記データを前記第一のプロファイル格納手段又は前記第二のプロファイル格納手段に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するスコア値算出手段と、
を備えることを特徴とする不正操作判定システム。
【請求項２】
前記第二のプロファイル作成手段は、前記コンピュータに特定のユーザがログインしている状態であるときに前記第二のプロファイルを作成すること
を特徴とする請求項１記載の不正操作判定システム。
【請求項３】
前記第一のプロファイル作成手段は、前記コンピュータに特定のユーザがログインしていない状態であるときに前記第一のプロファイルを作成すること
を特徴とする請求項２記載の不正操作判定システム。
【請求項４】
前記コンピュータにかかるログデータを格納する第一のログデータ格納手段と、
前記コンピュータにかかるユーザ別のログデータを格納する第二のログデータ格納手段と、を備えていて、
前記第一のプロファイル作成手段は、前記第一のログデータ格納手段を参照して前記第一のプロファイルを作成し、
前記第二のプロファイル作成手段は、前記第二のログデータ格納手段を参照して前記第二のプロファイルを作成すること
を特徴とする請求項１乃至３いずれかに記載の不正操作判定システム。
【請求項５】
前記コンピュータに特定のユーザがログインしているかを検出するための処理を実行するログイン検出手段を備えており、
前記ログイン検出手段により特定のユーザがログインしていることが検出されると、前記第二のプロファイル作成手段が前記ユーザにかかるプロファイルを作成すること
を特徴とする請求項１乃至４いずれかに記載の不正操作判定システム。
【請求項６】
前記ログイン検出手段が検出処理を実行しても特定のユーザがログインしていることが検出されない場合には、前記第一のプロファイル作成手段がプロファイルを作成すること
を特徴とする請求項５記載の不正操作判定システム。
【請求項７】
前記ログイン検出手段は、前記コンピュータが稼動している間は所定の間隔で検出処理を実行すること
を特徴とする請求項５又は６記載の不正操作判定システム。
【請求項８】
前記データから前記コンピュータを初めて操作するファーストユーザに対応する第三のプロファイルを作成する第三のプロファイル作成手段と、
前記第三のプロファイルを格納する第三のプロファイル格納手段と、を備えていて、

前記スコア値算出手段は、前記第二のプロファイル格納手段に換えて前記第三のプロファイル格納手段に格納された少なくとも一つのプロファイルを用いて前記オペレーションが不正操作であるかを判定すること
を特徴とする請求項１乃至７いずれかに記載の不正操作判定システム。
【請求項９】
前記コンピュータを操作するユーザの、前記コンピュータへのログイン回数、前記コンピュータを操作した操作時間、又は前記コンピュータを操作した操作日数の少なくとも一つの操作実績に関する累積値をユーザ別に格納する操作実績格納手段と、
前記操作実績格納手段を参照して、前記累積値が予め定められた基準値に満たない場合には、前記オペレーションを実行したユーザを、前記コンピュータを初めて操作するファーストユーザと判定するファーストユーザ判定手段と、を備えていて、
前記第三のプロファイル作成手段は、前記ファーストユーザ判定手段がファーストユーザと判定した場合に前記第三のプロファイルを作成し、
前記スコア算出手段は、前記ファーストユーザ判定手段がファーストユーザと判定した場合に前記第三のプロファイル格納手段に格納された少なくとも一つのプロファイルを用いて前記オペレーションが不正操作であるかを判定すること
を特徴とする請求項８記載の不正操作判定システム。
【請求項１０】
前記スコア値算出手段は、前記データと前記プロファイルの乖離計算によりスコア値を算出すること
を特徴とする請求項１乃至９いずれかに記載の不正操作判定システム。
【請求項１１】
前記スコア値が基準値を超えると前記オペレーションの停止処理を実行するオペレーション停止手段を備えること
を特徴とする請求項１乃至１０いずれかに記載の不正操作判定システム。
【請求項１２】
前記スコア値が基準値を超えると、前記コンピュータの操作画面に警告を表示、又は前記コンピュータに警告音を発生させるための処理を実行する警告処理手段を備えること
を特徴とする請求項１乃至１０いずれかに記載の不正操作判定システム。
【請求項１３】
前記スコア値が基準値を超えると、前記コンピュータの管理者が操作する管理サーバに不正操作の可能性を警告する通知を送信する警告通知送信手段を備えること
を特徴とする請求項１乃至１０いずれかに記載の不正操作判定システム。
【請求項１４】
コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定方法であって、
前記コンピュータが、前記オペレーションを実行するためのデータを受け付けるステップと、
前記コンピュータが、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納部に格納するステップと、
前記コンピュータが、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納部に格納するステップと、
前記コンピュータが、前記データを前記第一のプロファイル格納部又は前記第二のプロファイル格納部に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、
を有することを特徴とする不正操作判定方法。
【請求項１５】
コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定方法であって、
前記コンピュータが、前記オペレーションを実行するためのデータを受け付けるステップ

と、
前記コンピュータが、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納装置に送信するステップと、
前記コンピュータが、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納装置に送信するステップと、
前記コンピュータが、前記第一のプロファイル格納装置又は前記第二のプロファイル格納装置から少なくとも一つのプロファイルを取得して、前記データと前記プロファイルを対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、
を有することを特徴とする不正操作判定方法。
【請求項１６】
コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定プログラムであって、前記コンピュータに、
前記オペレーションを実行するためのデータを受け付けるステップと、
前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納部に格納するステップと、
前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納部に格納するステップと、
前記データを前記第一のプロファイル格納部又は前記第二のプロファイル格納部に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、
を実行させることを特徴とする不正操作判定プログラム。
【請求項１７】
コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定プログラムであって、前記コンピュータに、
前記オペレーションを実行するためのデータを受け付けるステップと、
前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納装置に送信するステップと、
前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納装置に送信するステップと、
前記第一のプロファイル格納装置又は前記第二のプロファイル格納装置から少なくとも一つのプロファイルを取得して、前記データと前記プロファイルを対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、
を実行させることを特徴とする不正操作判定プログラム。

【書類名】明細書
【発明の名称】不正操作判定システム、不正操作判定方法及び不正操作判定プログラム
【技術分野】
【０００１】
本発明は、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定システム、不正操作判定方法及び不正操作判定プログラムに関するものである。
【背景技術】
【０００２】
コンピュータに格納された情報の不正な取得やコンピュータからネットワークへの不正な侵入など、コンピュータの不正操作による被害を防止するために様々な技術が提供されている。例えば、ＩＤ・パスワード等により操作権限を認証する方法が広く用いられているが、この方法によるとＩＤ・パスワードを保有する権限のある者による不正操作や、ＩＤ・パスワードを不正に取得した第三者による操作などを防止することができない。
【０００３】
このような課題に対応するために、一般的に不正操作である可能性が高い操作パターンをルールとして登録し、コンピュータが受け付けた操作をルールと対比して不正操作である可能性を判定するルールベースによる判定が行われるようになっている。例えばネットワークに送出されるデータに対して、アクセス権や送信元、送信する文書の種類などについて予め定められたルールを参照して、不正の恐れがあると検知されると通信を切断する技術が開示されている（特許文献１参照。）。しかしながら、ルールベースによる判定は、不正な意図をもった操作であってもルールの範囲内であれば不正と判定されず、また、従来とは全く異なる方法により登録されたルールに該当しない不正な操作が実行されると、これを感知することができないという問題を有している。
【０００４】
そこで、一般に不正な操作は日常的に行われる操作とは異なり、あるタイミングにおいて特異に発生する操作であることに着目して、コンピュータに対する操作の履歴からユーザの行動パターンを設定したプロファイルを作成し、コンピュータが受け付けた操作をプロファイルと対比して不正操作である可能性を判定する方法も発明されている。例えば、ユーザのネットワークの使用状況からプロファイルを作成してネットワークの不正侵入を検知する技術や（特許文献２参照。）、コンピュータの操作履歴から日常的な操作内容を登録して、これに合致しない操作を不正操作と判定する技術が（特許文献３参照。）、開示されている。
【０００５】
【特許文献１】特開２００２－２３２４５１号広報
【特許文献２】特開２００２－１３５２４８号広報
【特許文献３】特開２００２－２５８９７２号広報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
前記特許文献２及び前記特許文献３記載の発明は、いずれもコンピュータの操作パターンはコンピュータのユーザ単位で設定されることとなっている。例えば企業等で業務用に用いられるコンピュータは、１台のコンピュータに複数のアカウントを設けて複数のユーザが共同で利用することが少なくないため、不正の基準となるプロファイルはユーザ単位で設定することが好ましい。しかしながら、ユーザ単位でプロファイルを設ける方式には、次のような課題が存在している。
【０００７】
まず、不正操作の判定を複数のコンピュータとネットワークで接続された管理用のサーバで行うこととした場合、あるユーザが自己のプロファイルの範囲内において操作を行う限りは、通常使用しているコンピュータと異なるコンピュータを操作していても正常な操

作であると判定されてしまうことになる。当該ユーザが何らかの不正を行うために同一のネットワーク上にあるが通常は使用しないコンピュータを使用していた場合、例えば、本社で会計関係のデータを扱っている権限のある社員が、通常は使わない倉庫のコンピュータで会計関係のデータを操作していた場合、特異な操作で不正の可能性があるにも関わらず、ユーザ単位のプロファイルのみではかかる操作を不正と判定することができない。

【０００８】

また、ユーザ単位でプロファイルを作成する場合、特定のコンピュータについて新しいユーザアカウントを設けた場合、新たなユーザについて信頼性の高いプロファイルを作成するためには、当該ユーザについて一定の操作履歴の蓄積を待たねばならず、その間は有効な判定を行うことができない、という問題もある。

【０００９】

これらの課題に対処するためには、不正操作の判定を行うためのプロファイルをユーザ単位でのみ設定するのではなく、コンピュータ単位でも設定して双方の観点から総合的に判定することが好ましい。かかる判定を行うためには、コンピュータが様々な操作を受け付ける中で、コンピュータ単位のプロファイルとユーザ単位のプロファイルを効率的に作成することが必要になる。

【００１０】

本発明は、このような課題に対応してなされたものであり、コンピュータが受付けたオペレーションを、コンピュータ単位のプロファイルとユーザ単位のプロファイルを参照して不正操作であるかを判定するための不正操作判定システム、不正操作判定方法及び不正操作判定プログラムを提供することを目的とするものである。

【課題を解決するための手段】

【００１１】

このような課題を解決するために、本発明は、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定システムであって、前記オペレーションを実行するためのデータを受け付けるオペレーション受付手段と、前記データから前記コンピュータにかかる第一のプロファイルを作成する第一のプロファイル作成手段と、前記第一のプロファイルを格納する第一のプロファイル格納手段と、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成する第二のプロファイル作成手段と、前記第二のプロファイルをユーザ別に格納する第二のプロファイル格納手段と、前記データを前記第一のプロファイル格納手段又は前記第二のプロファイル格納手段に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するスコア値算出手段と、を備えることを特徴とする。前記第二のプロファイル作成手段は、前記コンピュータに特定のユーザがログインしている状態であるときに前記第二のプロファイルを作成することを特徴とすることもできる。前記第一のプロファイル作成手段は、前記コンピュータに特定のユーザがログインしていない状態であるときに前記第一のプロファイルを作成することを特徴としてもよい。

【００１２】

この発明においては、コンピュータが受け付けたオペレーションからコンピュータ単位、ユーザ単位それぞれを基準にしたプロファイルを作成して格納し、新たに受け付けたオペレーションをそれぞれ対応するプロファイルと対比して不正操作の判定を行うことにより、ユーザを基準とした特異な操作からの判定のみでなく、コンピュータに対する特異な操作に対する判定を行うことができる。そのため、権限のあるユーザがコンピュータを換えて行う不正や、ユーザプロファイルの作成していない新規のユーザの不正にも対応することができる。

【００１３】

プロファイルの作成においては、特定のユーザのオペレーションをユーザＩＤ等で識別して、コンピュータに特定のユーザがログインしている状態でのオペレーションからはユーザ単位でのプロファイルを作成することとすればよい。コンピュータ単位でのプロファイルの作成は、特定のユーザがログインせずにコンピュータが操作されている状態でのオ

ペレーションのみを対象としてもよいし、特定のユーザがログインした状態も含めた全てのオペレーションを対象としてもよい。

【００１４】

また、本発明は、前記コンピュータにかかるログデータを格納する第一のログデータ格納手段と、前記コンピュータにかかるユーザ別のログデータを格納する第二のログデータ格納手段と、を備えていて、前記第一のプロファイル作成手段は、前記第一のログデータ格納手段を参照して前記第一のプロファイルを作成し、前記第二のプロファイル作成手段は、前記第二のログデータ格納手段を参照して前記第二のプロファイルを作成することを特徴とすることもできる。

【００１５】

コンピュータ単位のプロファイル、ユーザ単位でのプロファイルは、いずれもそれぞれコンピュータ、ユーザの操作傾向を定義するものなので、プロファイルの作成には過去の操作履歴であるログデータを用いることができる。

【００１６】

さらに、本発明は、前記コンピュータに特定のユーザがログインしているかを検出するための処理を実行するログイン検出手段を備えており、前記ログイン検出手段により特定のユーザがログインしていることが検出されると、前記第二のプロファイル作成手段が前記ユーザにかかるプロファイルを作成することを特徴とすることもできる。前記ログイン検出手段が検出処理を実行しても特定のユーザがログインしていることが検出されない場合には、前記第一のプロファイル作成手段がプロファイルを作成することを特徴としてもよい。前記ログイン検出手段は、前記コンピュータが稼動している間は所定の間隔で検出処理を実行することを特徴としてもよい。

【００１７】

このように構成すると、プロファイルの作成に用いられる特定のオペレーションが行われない場合であっても、ユーザがログインしていることが検出されるとその時点で当該ユーザがコンピュータを使用していることを、ログインしていない場合にもコンピュータが稼動していることを、操作履歴として記録することができる。このように記録される操作履歴は、稼働時間からユーザやコンピュータの操作傾向を分析して、プロファイルの作成に用いることができる。

【００１８】

さらに、本発明は、前記データから前記コンピュータを初めて操作するファーストユーザに対応する第三のプロファイルを作成する第三のプロファイル作成手段と、前記第三のプロファイルを格納する第三のプロファイル格納手段と、を備えていて、前記スコア値算出手段は、前記第二のプロファイル格納手段に換えて前記第三のプロファイル格納手段に格納された少なくとも一つのプロファイルを用いて前記オペレーションが不正操作であるかを判定することを特徴とすることもできる。　前記コンピュータを操作するユーザの、前記コンピュータへのログイン回数、前記コンピュータを操作した操作時間、又は前記コンピュータを操作した操作日数の少なくとも一つの操作実績に関する累積値をユーザ別に格納する操作実績格納手段と、前記操作実績格納手段を参照して、前記累積値が予め定められた基準値に満たない場合には、前記オペレーションを実行したユーザを、前記コンピュータを初めて操作するファーストユーザと判定するファーストユーザ判定手段と、を備えていて、

前記第三のプロファイル作成手段は、前記ファーストユーザ判定手段がファーストユーザと判定した場合に前記第三のプロファイルを作成し、前記スコア算出手段は、前記ファーストユーザ判定手段がファーストユーザと判定した場合に前記第三のプロファイル格納手段に格納された少なくとも一つのプロファイルを用いて前記オペレーションが不正操作であるかを判定することを特徴としてもよい。

【００１９】

ユーザプロファイルの作成されていないコンピュータを始めて使用するファーストユーザに対しては、操作するコンピュータのプロファイルから一般的な不正操作を判定するこ

とはできるが、このように構成すると、さらにファーストユーザの一般的な操作傾向と対比することにより、より正確な不正操作の判定を行うことができる。ファーストユーザとして扱うユーザは、当該コンピュータを全く初めて操作するユーザに限定してもよいが、適切なユーザプロファイルが作成されるまでは２回目以降についても当面の間は一般的なファーストユーザ用のプロファイルを用いることとしてもよい。ファーストユーザ用のプロファイルを用いる期間は、初回のみの他に、所定のログイン回数を指定、所定の操作時間を指定（例えば、合計ログイン時間９９時間等。）、所定の操作日数を指定（例えば、初回操作から１０日間の間等。）などのルールを自由に設定できることとしてもよい。

【００２０】

さらに、本発明は、前記スコア値算出手段は、前記データと前記プロファイルの乖離計算によりスコア値を算出することを特徴とすることもできる。

【００２１】

さらに、本発明は、前記スコア値が基準値を超えると前記オペレーションの停止処理を実行するオペレーション停止手段を備えることを特徴とすることもできる。前記スコア値が基準値を超えると、前記コンピュータの操作画面に警告を表示、又は前記コンピュータに警告音を発生させるための処理を実行する警告処理手段を備えることを特徴としてもよい。前記スコア値が基準値を超えると、前記コンピュータの管理者が操作する管理サーバに不正操作の可能性を警告する通知を送信する警告通知送信手段を備えることを特徴としてもよい。

【００２２】

このように、スコア値の算出は受け付けたオペレーションに関するデータと一般的な操作傾向であるプロファイルとの乖離計算により行うことが可能であり、不正操作であるか否かの判定は、スコア値が所定の基準値を超えるか否かにより行えばよい。不正操作と判定された場合には、オペレーションを中止させてもよいし、コンピュータに警告画面を表示したり警告音を発したりしてもよい。ネットワークを通じて管理者に不正の発生を通知してもよい。

【００２３】

本発明は、これまで説明した不正操作判定システムのそれぞれの構成を用いた不正操作判定方法として把握することもできる。また、不正操作判定システムのそれぞれの構成に用いられる不正操作判定プログラムとして把握してもよい。尚、上記の不正操作判定方法及び不正操作判定プログラムは、プロファイルをコンピュータ内に格納して不正操作の判定を行う場合、プロファイルをネットワークで接続された他のコンピュータに格納して判定を行う場合の２つのケースにより、各々の手順が異なることになる。

【００２４】

つまり、本発明にかかる第一の不正操作判定方法は、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定方法であって、前記コンピュータが、前記オペレーションを実行するためのデータを受け付けるステップと、前記コンピュータが、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納部に格納するステップと、前記コンピュータが、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納部に格納するステップと、前記コンピュータが、前記データを前記第一のプロファイル格納部又は前記第二のプロファイル格納部に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップとを有することを特徴とする不正操作判定方法である。

【００２５】

本発明にかかる第二の不正操作判定方法は、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定方法であって、前記コンピュータが、前記オペレーションを実行するためのデータを受け付けるステップと、前記コンピュータが、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納装置に送信するステップと、前記コンピュータが、前記データから前記コン

ピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納装置に送信するステップと、前記コンピュータが、前記第一のプロファイル格納装置又は前記第二のプロファイル格納装置から少なくとも一つのプロファイルを取得して、前記データと前記プロファイルを対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、を有することを特徴とする不正操作判定方法。

【００２６】

また、本発明にかかる第一の不正操作判定プログラムは、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定プログラムであって、前記コンピュータに、前記オペレーションを実行するためのデータを受け付けるステップと、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納部に格納するステップと、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納部に格納するステップと、前記データを前記第一のプロファイル格納部又は前記第二のプロファイル格納部に格納された少なくとも一つのプロファイルと対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、を実行させることを特徴とする不正操作判定プログラムである。

【００２７】

本発明にかかる第二の不正操作判定プログラムは、コンピュータが受付けたオペレーションが不正操作であるかを判定するための不正操作判定プログラムであって、前記コンピュータに、前記オペレーションを実行するためのデータを受け付けるステップと、前記データから前記コンピュータにかかる第一のプロファイルを作成して、第一のプロファイル格納装置に送信するステップと、前記データから前記コンピュータを操作するユーザ別の第二のプロファイルを作成して、第二のプロファイル格納装置に送信するステップと、前記第一のプロファイル格納装置又は前記第二のプロファイル格納装置から少なくとも一つのプロファイルを取得して、前記データと前記プロファイルを対比して前記オペレーションが不正操作であるかを判定するためのスコア値を算出するステップと、を実行させることを特徴とする不正操作判定プログラムである。

【発明の効果】

【００２８】

本発明により、ルールベースでは判定できないコンピュータに対する特異な操作について不正操作であるか否かを判定できるとともに、ユーザを基準とした特異な操作からの判定のみでなく、コンピュータに対する特異な操作に対する判定を行うことも可能になる。そのため、権限のあるユーザがコンピュータを換えて行う不正や、ユーザプロファイルの作成されていない新規のユーザの不正にも対応することができるので、コンピュータの不正操作に対する安全性を著しく高めることができる。

【発明を実施するための最良の形態】

【００２９】

本発明を実施するための最良の形態について、図面を用いて以下に詳細に説明する。尚、以下の説明では主としてネットワークに接続されたコンピュータの不正操作を判定する例について説明するが、これは本発明の実施形態の一例であって、コンピュータはスタンドアローンで用いられるものであってもよく、本発明はかかる実施形態に限定されるものではない。

【００３０】

図１は、本発明にかかる不正操作判定システムの概要を示す図である。図２、図３は、本発明にかかる不正操作判定システムの、それぞれ第１、第２の実施形態を示すブロック図である。図４は、本発明にかかる不正操作判定システムの構成を示すブロック図である。図５、図６は、本発明にかかる不正操作判定システムにより、ノードプロファイルとユーザプロファイルの作成する、それぞれ第１、第２のパターンを示す図である。図７は、本発明にかかる不正操作判定システムのフローを示すフローチャートである。

【００３１】

図１を用いて、本発明にかかる不正操作判定システムの概要について説明する。図１の例では、本発明にかかる不正操作判定システムはネットワークに接続されたクライアントＰＣに備えられている。クライアントＰＣは複数のユーザにより利用されていて、各々のユーザに対応したアカウントが設けられている。

【００３２】

あるユーザがクライアントＰＣで何らかのオペレーションを実行すると、当該クライアントＰＣが受け付けるオペレーションの傾向及び当該ユーザの実行するオペレーションの傾向を学習してそれぞれノードプロファイル、ユーザプロファイルを作成する。このように作成されたプロファイルは、ノードプロファイルはノードプロファイルステートテーブルに、ユーザプロファイルは各々のユーザについて設けられたユーザプロファイルステートテーブルに、それぞれ格納される。

【００３３】

当該ユーザが実行したオペレーションについてプロファイルを作成すると、次に当該オペレーションが特異操作に該当するか否かの判定が行われる。判定はノードプロファイルステートテーブルに格納されたノードプロファイル、ユーザプロファイルステートテーブルに格納された対応するユーザのユーザプロファイルを参照して、通常の操作パターンとの乖離計算により実行される。参照するテーブルは、オペレーションの内容によってノードプロファイル、ユーザプロファイルの双方であってもよいし、いずれか一方であってもよい。

【００３４】

乖離計算の結果は、不正操作の可能性を示すスコア値として算出される。スコア値に一定の基準値を設けることにより、基準値を超えて不正操作である可能性が高いオペレーションに対しては、オペレーションの中止処理、ディスプレイへの警告表示、管理者への通知の送信など、予め定められたアクションを実行するよう設定することができる。

【００３５】

本発明にかかる不正操作判定システムは、コンピュータをスタンドアローンで用いる場合、コンピュータをネットワークに接続して用いる場合のいずれにおいても利用することができる。後者については、クライアントＰＣが単独で不正操作の判定を行うこととしてもよいし、クライアントＰＣが不正監視用のサーバと協働して不正操作の判定を行うこととしてもよい。図２は、クライアントＰＣが単独で不正操作の判定を行う本発明にかかる不正操作判定システムの第１の実施形態を、図３は、クライアントＰＣが不正監視用のサーバと協働して不正操作の判定を行う本発明にかかる不正操作判定システム第２の実施形態を示している。

【００３６】

図２に示した本発明にかかる不正操作判定システムは、ユーザ端末２０の処理装置２１０に備えられていて、ユーザ端末２０において受け付けたオペレーションが不正操作であるか否かを判定する。不正操作判定システムの機能は、処理装置２１０のＨＤＤ２１４に格納された学習プログラム１０及び不正判定プログラム１１により実行される。尚、処理装置においてプログラムを格納するＨＤＤ２１４については、フラッシュメモリなどプログラムを格納することができるその他の記憶媒体を用いるものであってもよい。

【００３７】

まず、ユーザ端末２０に電源が入れられると、ＲＯＭ２１３に記憶された入力制御や出力制御などのハードウェア制御のための基本的な各種プログラムを起動するとともに、ＨＤＤ２１４からコンピュータのオペレーションシステムを読み出して起動する。併せて、ＨＤＤ２１４から学習プログラム１０及び不正判定プログラム１１を読み出して起動し、ＲＡＭ２１２をワークエリアとして機能させながら、ＣＰＵ２１１が演算処理を行う。

【００３８】

学習プログラム１０及び不正判定プログラム１１は、例えばＩＤＥへの書き出しを何らかのオペレーションが実行されたイベントと捉えることにより、これらのイベントについて学習及び不正判定の処理を実行する。外部接続バス２２に書き出されたデータを監視し

て、出力装置２３や外部記憶装置２４に対して実行されるオペレーションとして、学習及び不正判定の処理を実行してもよい。処理装置２１０においてネットワークへの送信処理がされるデータを監視して、これらのデータを監視してネットワークとの送受信に関する学習及び不正判定の処理を実行してもよい。

【００３９】

学習については、受け付けたオペレーションをログデータ格納部１４に格納されたログと対比してオペレーションの傾向を分析し、分析結果からプロファイルを作成して、ユーザ端末２０に対するユーザを特定しない操作全体のプロファイルはノードプロファイル格納部１２に、ユーザを特定したプロファイルについてはユーザプロファイル格納部１３に格納する。不正判定については、ユーザ端末２０に対する一般的な判定についてノードプロファイル格納部１２を参照し、個々のユーザに対する判定についてユーザプロファイル格納部１３を参照する。

【００４０】

このように、不正操作の判定に用いられるプロファイルを格納するノードプロファイル格納部１２及びユーザプロファイル格納部１３はユーザ端末２０の内部に設けられていてもよいが、図３に示した第２の実施形態のように、ユーザ端末２０とネットワークで接続された不正監視サーバ３０のＨＤＤ３１４に設けられていてもよい。本発明にかかる不正操作判定システムは、プロファイルを用いた判定の他に一般的なルールベースの判定を併用してもよいが、第２の実施形態においては、例えば不正監視サーバ３０に複数のユーザ端末を接続して多くのプロファイルを蓄積し、これらのプロファイルからネットワーク内において汎用的に用いられるルールを作成して、汎用ルール格納部１６に格納することとしてもよい。また、図３の例には示していないが、学習プログラム１０や不正判定プログラム１１の機能を、不正監視サーバ３０側に設けることもできる。

【００４１】

図４を用いて、本発明にかかる不正操作判定システムにおけるそれぞれの機能の関連について説明する。まず、ユーザ端末２０に対して何らかのオペレーションが実行されると、当該オペレーションを実行するためのデータをデータ学習部１００が受け付ける。データ学習部１００は、ログデータ格納部１４を参照して、特異操作判定の基準となるプロファイルを作成する。

【００４２】

当該オペレーションが電源のオン・オフなど、ユーザアカウントにログインしていない状態でのオペレーションである場合には、ログデータ格納部１４ではユーザを特定しないユーザ端末２０についての一般的なログを参照し、データ学習部１００はユーザを特定しないユーザ端末２０についての一般的なプロファイルを作成して、ノードプロファイル格納部１２に格納する。

【００４３】

一方、当該オペレーションが特定のユーザアカウントにログインした後のオペレーションである場合には、ログデータ格納部１４では当該アカウントに対応するユーザをユーザＩＤ等で特定し、該当するユーザのログを参照し、データ学習部１００はユーザを特定したプロファイルを作成して、ユーザプロファイル格納部１３の該当するユーザに関するテーブルに格納する。尚、ユーザが特定されたオペレーションについては、これも同一のコンピュータが受け付けたオペレーションであるとして、併せてユーザを特定しないユーザ端末２０についての一般的なプロファイルを作成し、ノードプロファイル格納部１２に格納することとしてもよい。

【００４４】

次に、当該オペレーションを実行するためのデータは、特異操作判定部１１０において対応するプロファイルを参照して、不正操作である可能性についての判定が行われる。当該オペレーションがユーザを特定しない操作である場合には、ノードプロファイル格納部１２に格納されたプロファイルを、当該オペレーションがユーザを特定することができる操作である場合には、ユーザプロファイル格納部１３に格納された対応するユーザのプロ

ファイルを参照して、特異操作であるか否かの判定が行われる。

【００４５】

特異操作の判定は、受け付けたオペレーションと対応するプロファイルの乖離計算により行われる。乖離計算の基準には、例えばオペレーションを受け付ける時間帯やその標準値、オペレーションの頻度、処理に要するデータ量など、数値化の可能な様々なデータを用いることができる。

【００４６】

特異操作判定部１１０において乖離計算が実行されると、スコア算出部１１１においては不正操作である可能性をスコア値として算出する。スコアの設定は乖離計算により算出されたプロファイルとの乖離度合いにより定めることとすればよいが、算出されたスコアに一定の基準値を設けることにより、基準値を上回る場合には不正操作であると判定して、オペレーションの中止処理等を実行するよう設定することもできる。

【００４７】

尚、上記で説明したデータ学習部１００、特異操作判定部１１０、スコア算出部１１１の各部は物理的に分離されて設けられたものではなく、各々の処理を実行するためのプログラムとしてＨＤＤ２１４に格納された学習プログラム１０又は不正判定プログラム１１に含まれていて、順次読み出されてＲＡＭ２１２をワークエリアとして機能させながら、ＣＰＵ２１１により演算処理が実行されるものである。

【００４８】

また、上記の説明では、オペレーションを受け付けると学習を行った後に特異判定を行うこととしているが、処理の順序はこのように限定されるものではなく、受け付けたオペレーションの特異判定を行った後に、当該オペレーションに関する学習を行って新たなプロファイルを作成することとしてもよい。

【００４９】

次に、図５、図６を用いて、本発明にかかる不正操作判定システムによりノードプロファイルとユーザプロファイルを作成する手順について、具体例に沿って２つのパターンを説明する。図５は、ユーザが特定されていない場合のオペレーションについてはノードプロファイルを、ユーザが特定されている場合のオペレーションについてはユーザプロファイルを作成する第１のパターンを示す図である。図６は、全てのオペレーションについてノードプロファイルを、ユーザが特定されている場合のオペレーションについてはユーザプロファイルを作成する第２のパターンを示す図である。

【００５０】

図５に示した第１のパターンにおいて、コンピュータに電源が入れられてオペレーションシステムが起動された後に、本発明にかかる不正操作判定システムが起動される。ここでコンピュータに電源を入れるというオペレーションをイベントとして捉え、コンピュータの起動時間等に関するプロファイルを作成するが、この時点ではユーザがログインしておらず特定できないため、当該コンピュータに関する一般的なプロファイルとしてノードプロファイルが作成される。

【００５１】

次に、コンピュータを起動したユーザ１が自らのアカウントにログインすると、ユーザ１がログインしたというオペレーションをイベントとして、ユーザ１に関するプロファイルを作成する。ユーザ１がログイン中に行ったアプリケーションの起動や操作、ネットワークへのアクセス、プリントアウト等の様々なオペレーションもイベントとして捉えることが可能であり、これらのイベントからもユーザ１に関するプロファイルが作成される。ユーザ１がログアウトすると、ログアウトについてもユーザ１のプロファイルを作成することができる。

【００５２】

ユーザ１がログアウトした後、他のユーザがログインするまでの間に、電源のオン・オフその他のオペレーションが行われた場合には、ユーザが特定されないオペレーションとしてノードプロファイルが作成される。その後にユーザ２がログインすると、ユーザ１の

場合と同様に、ユーザ２についてのプロファイルが作成される。ユーザ２のプロファイルは、ユーザＩＤ等によりユーザ１のプロファイルと識別して格納される。

【００５３】

コンピュータが受け付けたオペレーションの不正操作の判定においては、上記の区分と同様に、ユーザが特定されていない状態ではノードプロファイルが、ユーザが特定されている状態では各々のユーザに対応するユーザプロファイルが用いられる。各々のユーザに対応するプロファイルの特定は、ログイン時に受け付けたユーザＩＤ等を用いることができる。

【００５４】

図６に示した第２のパターンにおいては、ユーザが特定された状態で受け付けたオペレーションについて、各々のユーザのプロファイルを作成するとともに、ユーザを特定しない当該コンピュータについてのノードプロファイルを作成することとしている。ユーザが特定されたオペレーションであっても、当該コンピュータが受け付けたオペレーションであることに違いはないため、ノードプロファイルについては電源オンからオフまでの全てのオペレーションを対象にしてもよい。

【００５５】

また、プロファイルを作成する対象となるオペレーションは実行されていないが、コンピュータに電源が入れられた状態や、特定のユーザがログインした状態が継続していることをプロファイルの作成に用いることとしてもよい。そのためには、例えば１時間に１度といった頻度で当該処理を行うプログラムを起動して電源がオンであること、特定のユーザがログインしていることを検出し、これらの結果からプロファイルを作成するよう構成することもできる。

【００５６】

尚、これまで説明した図５及び図６いずれのパターンにおいても、ログインしているのは１ユーザという前提となっているが、オペレーションシステムにおいて１つのコンピュータに対して複数のログインが可能な設定が行われているなど、同時に複数ユーザの操作が並行して行われる場合においては、ユーザプロファイルの作成、ユーザプロファイルを用いた不正操作の判定についても、複数のユーザプロファイルを対象にした処理が同時に行われるよう設定することができる。ノードプロファイルについても、それぞれのユーザの全てのオペレーションを対象に、プロファイルの作成及びプロファイルによる判定を並行して処理することとしてもよい。

【００５７】

図７のフローチャートを用いて、本発明にかかる不正操作判定システムのフローについて説明する。尚、以下に説明するフローは、本発明にかかる不正操作判定システムの処理フローの一例であって、プロファイルの作成とスコア算出の順序、ユーザが特定されたオペレーションについてノードプロファイル作成の有無などについて、本発明は以下のフローに示した例に限定されるものではない。

【００５８】

まず、コンピュータに電源が入れられて不正操作判定システムが起動すると、コンピュータの起動についてのノードプロファイルを作成する（Ｓ０１）。作成されたノードプロファイルは、ノードプロファイルステートテーブルに格納される（Ｓ０２）。

【００５９】

次に、コンピュータの起動について、当該電源オンにかかるオペレーションとノードプロファイルステートテーブルに格納されたコンピュータの電源オンに関するノードプロファイルを対比して乖離計算を実行し（Ｓ０３）、スコアを算出する（Ｓ０４）。算出されたスコアを予め定められた基準値と対比して（Ｓ０５）、基準値を上回る場合には不正操作である可能性が高いとして、オペレーションの停止処理、具体的にはコンピュータの起動処理の停止を実行する（Ｓ０６）。

【００６０】

一方、スコアが基準値に満たない場合には、そのままオペレーションの受け付けが継続

される。特定のユーザについてのログインを受け付けると（Ｓ０７）、ログインしたユーザのユーザＩＤを識別する（Ｓ０８）。当該ユーザがログインを行ったことについてユーザプロファイルを作成し（Ｓ０９）、当該ユーザのユーザＩＤに対応するユーザプロファイルステートテーブルに、作成したユーザプロファイルを格納する（Ｓ１０）。

【００６１】

次に、当該ユーザのログインについて、当該ユーザのログインにかかるオペレーションと当該ユーザに対応するユーザプロファイルステートテーブルに格納されたログインに関するユーザプロファイルを対比して乖離計算を実行し（Ｓ１１）、スコアを算出する（Ｓ１２）。算出されたスコアを予め定められた基準値と対比して（Ｓ１３）、基準値を上回る場合には不正操作である可能性が高いとして、オペレーションの停止処理、具体的にはログインの受け付け処理の停止を実行する（Ｓ１４）。

【００６２】

一方、スコアが基準値に満たない場合には、そのままオペレーションの受け付けが継続される。ログインしたユーザは様々なアプリケーション等の処理を実行するが、不正操作判定システムは新たなアプリケーション等の起動をＩＤＥへの書き出しを監視することにより検出する（Ｓ１５）。ＩＤＥへの書き出しがない場合は監視を継続し、ＩＤＥへの書き出しが検出されると、書き出されたデータにより実行される処理に関するユーザプロファイルを作成し（Ｓ１６）、当該ユーザのユーザＩＤに対応するユーザプロファイルステートテーブルに、作成したユーザプロファイルを格納する（Ｓ１７）。尚、アプリケーション等の起動はＩＤＥへの書き出しを監視することにより検出することとしているが、アプリケーション等のワークエリアとなるメモリ領域を監視して、新たな操作が行われたことを検出することとしてもよい。

【００６３】

次に、当該ユーザのログインについて、当該ユーザのアプリケーションの起動等にかかるオペレーションと当該ユーザに対応するユーザプロファイルステートテーブルに格納されたアプリケーションの起動等に関するユーザプロファイルを対比して乖離計算を実行し（Ｓ１８）、スコアを算出する（Ｓ１９）。算出されたスコアを予め定められた基準値と対比して（Ｓ２０）、基準値を上回る場合には不正操作である可能性が高いとして、オペレーションの停止処理、具体的にはアプリケーションの中止処理等を実行する（Ｓ２１）。一方、スコアが基準値に満たない場合には、引続きＩＤＥへの書き出しの監視が継続される（Ｓ１５）。

【図面の簡単な説明】

【００６４】

【図１】本発明にかかる不正操作判定システムの概要を示す図である。

【図２】本発明にかかる不正操作判定システムの、第１の実施形態を示すブロック図である。

【図３】本発明にかかる不正操作判定システムの、第２の実施形態を示すブロック図である。

【図４】本発明にかかる不正操作判定システムの構成を示すブロック図である。

【図５】本発明にかかる不正操作判定システムにより、ノードプロファイルとユーザプロファイルの作成する第１のパターンを示す図である。

【図６】本発明にかかる不正操作判定システムにより、ノードプロファイルとユーザプロファイルの作成する第２のパターンを示す図である。

【図７】本発明にかかる不正操作判定システムのフローを示すフローチャートである。

【符号の説明】

【００６５】

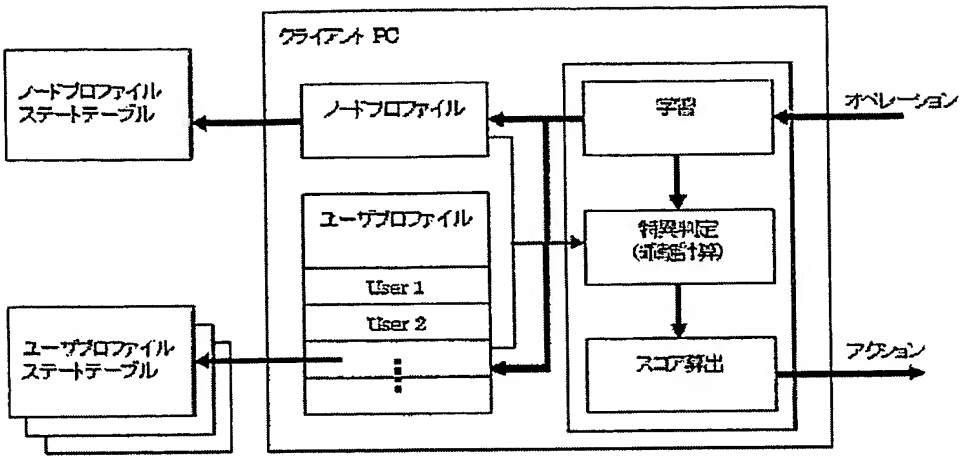
１０　　学習プログラム

１００　データ学習部

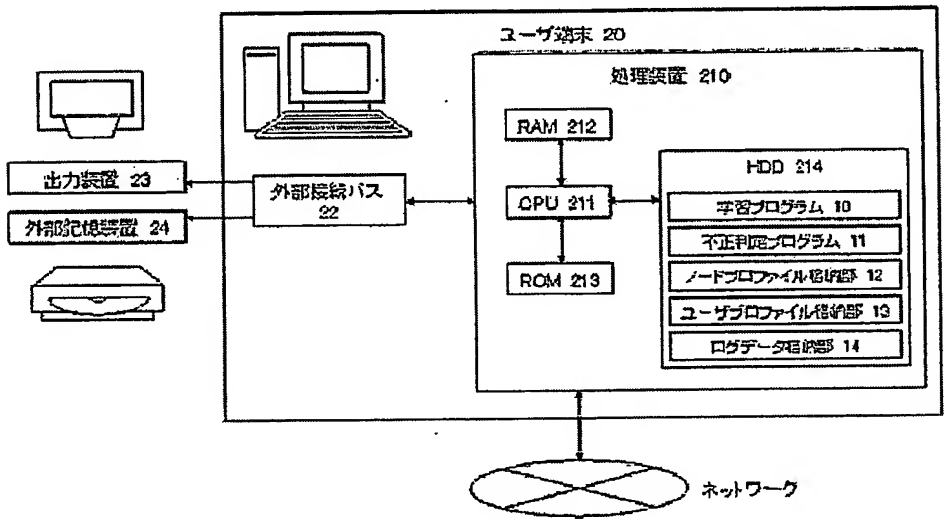
１１　　不正判定プログラム

１１０　特異操作判定部
１１１　スコア算出部
１２　　ノードプロファイル格納部
１３　　ユーザプロファイル格納部
１４　　ログデータ格納部
１５　　ログデータ格納部
１６　　汎用ルール格納部
２０　　ユーザ端末
２１０　処理装置
２１１　ＣＰＵ
２１２　ＲＡＭ
２１３　ＲＯＭ
２１４　ＨＤＤ
２２　　外部接続バス
２３　　出力装置
２４　　外部記憶装置
３０　　不正監視サーバ
３１１　ＣＰＵ
３１２　ＲＡＭ
３１３　ＲＯＭ
３１４　ＨＤＤ

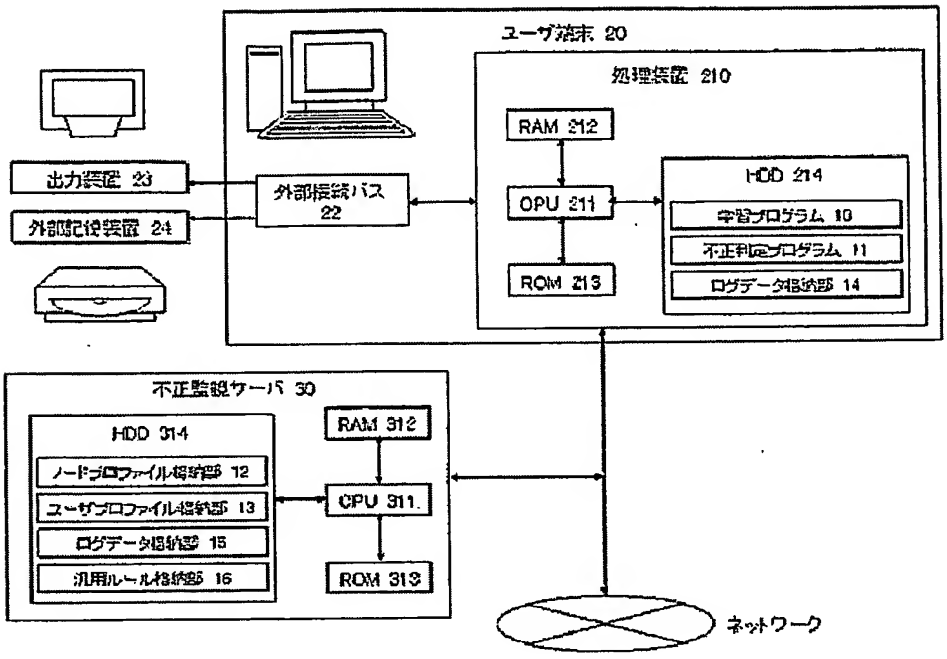
【書類名】図面
【図１】


クライアント PC
ノードプロファイル
ステートテーブル
ノードプロファイル
学習
オペレーション
ユーザプロファイル
User 1
User 2
特異判定
(距離計算)
ユーザプロファイル
ステートテーブル
スコア算出
アクション

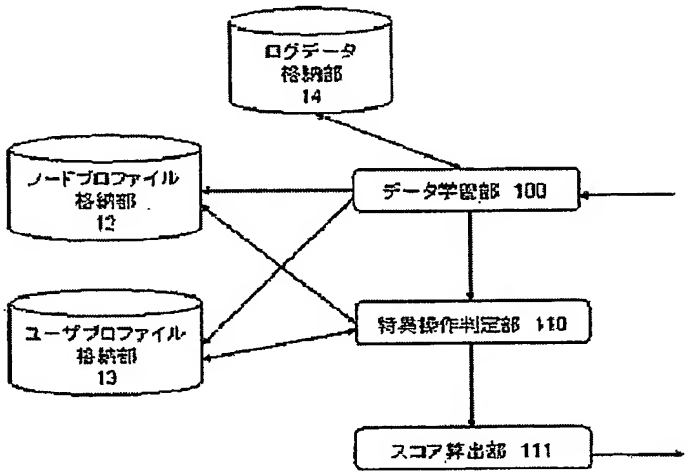
【図２】


ユーザ端末 20
処理装置 210
RAM 212
HDD 214
出力装置 23
外部接続バス
22
CPU 211
学習プログラム 10
不正判定プログラム 11
ノードプロファイル格納部 12
ユーザプロファイル格納部 13
ログデータ格納部 14
外部記憶装置 24
ROM 213
ネットワーク

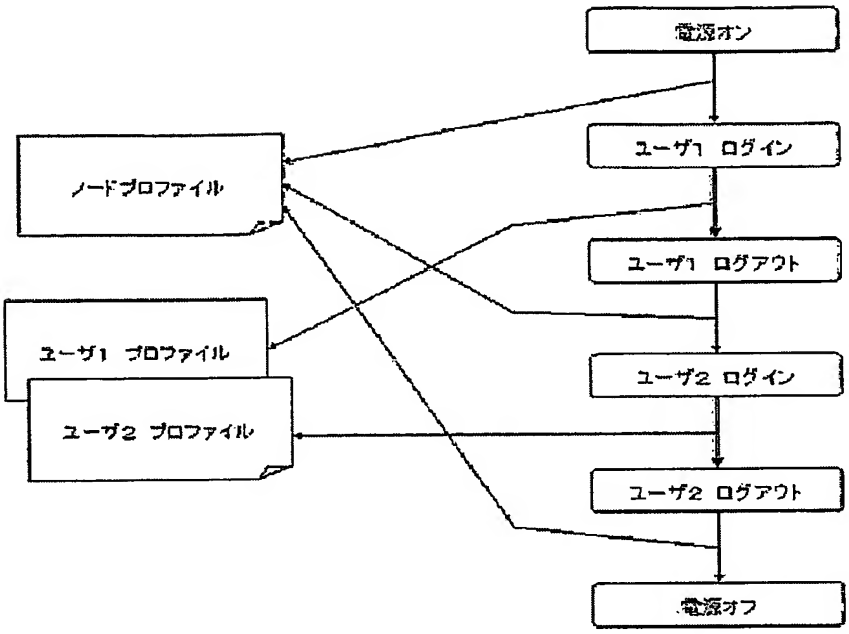
【図３】


ユーザ端末 20
処理装置 210
RAM 212
CPU 211
ROM 213
HDD 214
学習プログラム 10
不正判定プログラム 11
ログデータ格納部 14
出力装置 23
外部記憶装置 24
外部接続バス 22
不正監視サーバ 30
HDD 314
ノードプロファイル格納部 12
ユーザプロファイル格納部 13
ログデータ格納部 15
汎用ルール格納部 16
RAM 312
CPU 311
ROM 313
ネットワーク

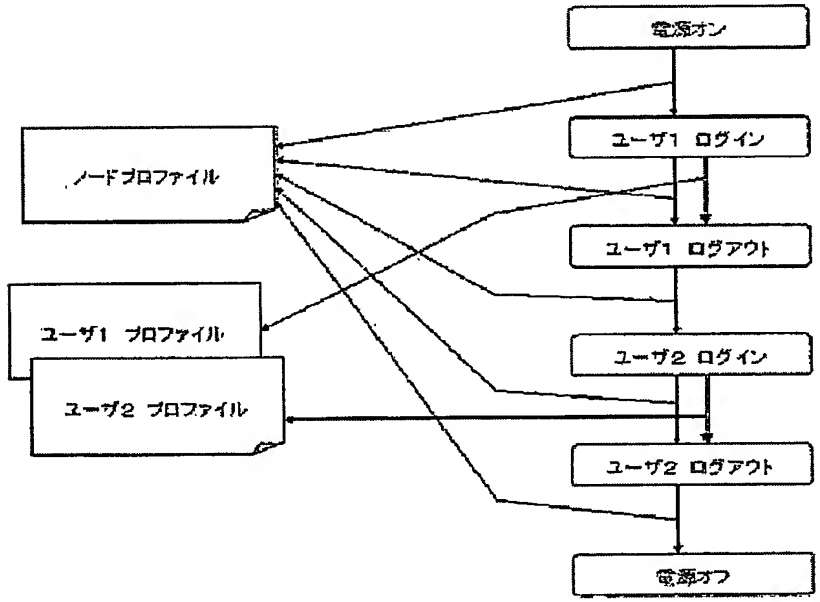
【図４】


ログデータ格納部 14
ノードプロファイル格納部 12
ユーザプロファイル格納部 13
データ学習部 100
特異操作判定部 110
スコア算出部 111

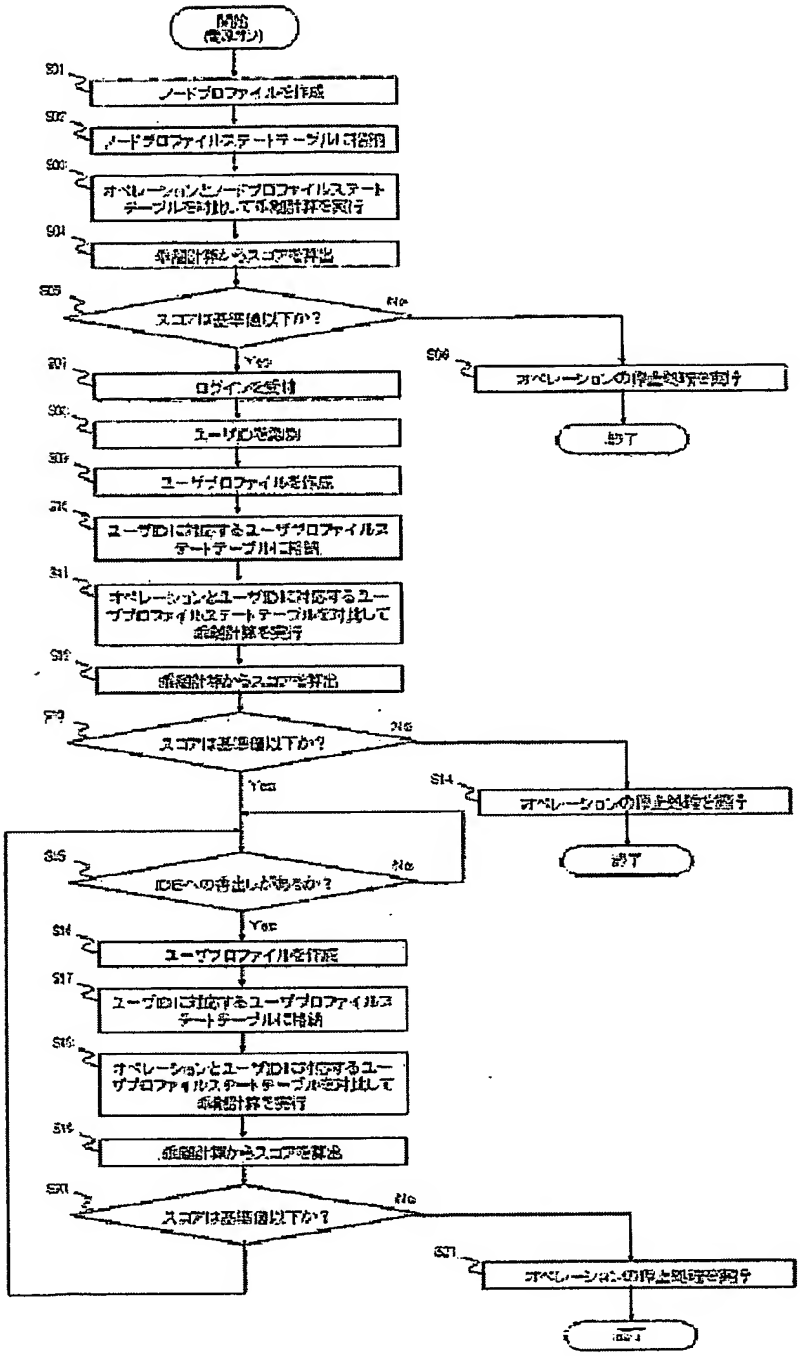
【図５】


電源オン
ユーザ1 ログイン
ノードプロファイル
ユーザ1 ログアウト
ユーザ1 プロファイル
ユーザ2 ログイン
ユーザ2 プロファイル
ユーザ2 ログアウト
電源オフ

【図６】


電源オン
ユーザ1 ログイン
ノードプロファイル
ユーザ1 ログアウト
ユーザ1 プロファイル
ユーザ2 ログイン
ユーザ2 プロファイル
ユーザ2 ログアウト
電源オフ

【図７】


開始
(電源オン)
S01
ノードプロファイルを作成
S02
ノードプロファイルステートテーブルに登録
S03
オペレーションとノードプロファイルステートテーブルを対比して相関計算を実行
S04
相関計算からスコアを算出
S05
スコアは基準値以下か?
No
Yes
S06
オペレーションの停止処理を実行
終了
S01
ログインを受付
S02
ユーザIDを識別
S07
ユーザプロファイルを作成
S08
ユーザIDに対応するユーザプロファイルステートテーブルに登録
S11
オペレーションとユーザIDに対応するユーザプロファイルステートテーブルを対比して相関計算を実行
S12
相関計算からスコアを算出
S13
スコアは基準値以下か?
No
Yes
S14
オペレーションの停止処理を実行
終了
S15
IDEへの呼出しがあるか?
No
Yes
S16
ユーザプロファイルを作成
S17
ユーザIDに対応するユーザプロファイルステートテーブルに登録
S18
オペレーションとユーザIDに対応するユーザプロファイルステートテーブルを対比して相関計算を実行
S19
相関計算からスコアを算出
S20
スコアは基準値以下か?
No
S21
オペレーションの停止処理を実行
終了

【書類名】要約書
【要約】
【課題】　コンピュータが受付けたオペレーションについて、プロファイルを参照して特異行動から不正操作であるかを判定するための不正操作判定システムを提供する。権限のあるユーザがコンピュータを換えて行う不正や、ユーザプロファイルの作成されていない新規ユーザの不正にも対応する。
【解決手段】　ユーザがあるオペレーションを実行すると、当該オペレーションの傾向及び当該ユーザの実行するオペレーションの傾向を学習してそれぞれノードプロファイル、ユーザプロファイルを作成し、それぞれノードプロファイルステートテーブル、各々のユーザのユーザプロファイルステートテーブルに格納される。このように作成されたノードプロファイル、ユーザプロファイルを参照して、受け付けたオペレーションと通常の操作パターンとの乖離計算を行って、当該オペレーションが特異操作に該当するか否かを判定し、不正操作である可能性をスコア値として算出する。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３８７２１３
受付番号	５０３０１８９８９１２
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年１１月１８日

＜認定情報・付加情報＞

【提出日】　平成15年11月17日

特願２００３－３８７２１３

出　願　人　履　歴　情　報

識別番号　［３９７０６７８５３］

１．変更年月日　１９９７年１０月２８日
［変更理由］　新規登録
住　所　東京都江東区木場５丁目１２番８号
氏　名　株式会社インテリジェントウェイブ